A New Steganography Method for Hiding Message in Image Based on Quad Chain Code and DCT

[1]Prof. Dr. Tawfiq A. Al-asadi, [2]Prof. Dr. Israa Hadi Ali,
[3]Abdul kadhem Abdul kareem Abdul kadhem
[1,2,3] *Information Technology College/ Babylon University, Iraq.*
[1] tawfiqasadi63@yahoo.com; [2] israa_hadi1968@yahoo.com; [3] kazum2006k@yahoo.com

Abstract

*In this paper we present new approach for information hiding based on quad chain code (QCC) and Discrete Cosine Transform (DCT). The proposed system consists of two general stages. The first one is hiding the secret message in the cover image that consist of many steps, the first step is applying quad chain code for the cover, the second step is equipment block with size 8*8 pixels that were more alike with each other, the third step is applying the 2D-DCT transform for a block and applying the signature of coefficients algorithm that was used to find number of bits can be embedded in the block, the fourth step is hide number of bits (message) in some locations of block depending on the above step, the fifth step is save the (start point of quad chain code, stream of chain code, number of bits) in the boundary of the stego image and reconstruct the block in the stego image, finally check if there are bits still not hidden in the message and check if there are blocks with more similarity to return the above steps. The second stage is extracting the secret message from the stego image that consist of number of steps, the first step is determining the (number of blocks, stream of chain code, number of bits for each block) from boundary of the stego image, this information are helping to extract the message in the next steps .*

Keywords: *Information Hiding, Steganography, Chain code, DCT.*

1. Introduction

Security of information is important in of information technology and communication because of the large use of World Wide Web. Cryptography was developed as a way of securing information of all kinds. Information hiding is one of the important methods that are used in security fields and Steganography is a technique of this kind of security [1]. This technique hides secret information within a normal type of media, such as digital image, audio, video, etc. any strange attempt to detect and extract the hidden secret information from stego is known as steganalysis. If any steganalytic algorithm detect a given media is a carrier then the steganographic algorithm is considered to be broken [2]. The main goal of steganography is to communicate securely that the real message is invisible to the observer. That is unwanted parties should not be able to distinguish between the cover-image (which is the image without any secret message) and stego-image (the image that is modified to contain the secret message) [3]. Some of the technologies that are near to steganography are watermarking and fingerprinting. These technologies are referring to the protection of intellectual property. To provide security, many techniques have been used in past research. Steganography is a great science of hiding communication [4]. There are many applications for steganography which are military, diplomatic and personal applications, in high secured information in ministries. There are three ideologies to determine the effectiveness of steganography technique which are (The size of a message, the difficulty of detect message, the difficulty of changing the message). Steganography can be categorized into three kinds: (1) Pure steganography which hide information (message) directly in a cover in a deterministic sequence without use key so this sequence is known to the sender and receiver.(2) Symmetric key steganography which hide a message in a cover by using a secret key and the key is known to the sender and receiver. (3) Public key steganography which hide message in a cover by using two keys: secret key which is used in hiding and a public key which is used in extracting the message [5].

The secret message can be hidden inside the cover image in some locations that depends on Chain code. Chain codes are one of the shape representations which refer to represent a boundary by a connected sequence of straight line segments of identified length and direction. This representation is based on 4- connectivity or 8-connectivity of the segments [6]. There are two basic methods that were implemented in steganography: Least significant bit (LSB) that is used in Spatial Domain Technique and

Transform-based (DCT) that is used in Frequency Domain Technique. LSB steganography is a one of the easiest methods. Data hidden in images using this method is highly sensitive to image alteration and vulnerable to attack. DCT steganography is potentially more resistant to loss from image manipulation and increases the difficulty to a potential attacker [8].

2. Related Work.

Zuheir H. Ali [9] proposed a steganography method to hide text in the cover image by using traditional chain code, where first generate a chain code and store it in the image then store the embedded text in the image according to the generated chain code .the system using the first pixel in the image to specify the location of starting point to begin with it, The second pixel contain the length of secret message where each character need 8 bits for representation. We divided the image into two sections the first half contain the chain code which represent the map of secret message and the second half include the secret message which the sender pass.

A.Nag, S. Biswas, D. Sarkara and P.P. Sarkar [2] presented a novel technique for Image steganography based on Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain. Firstly a gray level image of size M× N is divided into no joint 8×8 blocks and a two-dimensional Discrete Cosine Transform (2-d DCT) is performed on each of the blocks. Then Huffman encoding is also performed on the secret messages before embedding and each bit of Huffman code of secret message is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks.

K B Shiva Kumar, K B Raja, R K Chhotaray and Sabyasachi Pattanaik [10] proposed method by using Bit Length Replacement Steganography using Segmentation and DCT. The cover image is segmented into smaller matrix of size 8×8 and converted to DCT domain. The MSB bits of payload in the spatial domain are embedded into each DCT coefficients of the cover image based on the coherent length L which is determined by the DCT coefficient values.

Shahana T [11] implements the steganography in the frequency domain by using DCT. In this method, the cover image is transformed from the spatial domain to the frequency domain using 2D DCT. Then the secret image is encrypted using RSA algorithm and it is embedded in the cover image to obtain the stego image. To extract the secret image apply 2D DCT on stego image and apply the decryption algorithm. According to the simulation results, the stego images of our proposed algorithm are almost identical to the cover images and it is very difficult to differentiate between them.

3. Background.

3.1. Chain code.

Chain code was introduced by Freeman in 1961 so it is known by his name as Freeman chain code (FCC). This code follows the contour in counter Clockwise manner and keeps track of the directions as we go from one contour pixel to the next. The codes involve 4–connected and 8–connected paths As Shown in figure 1. [6,7].

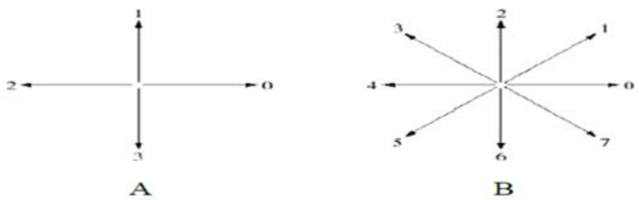
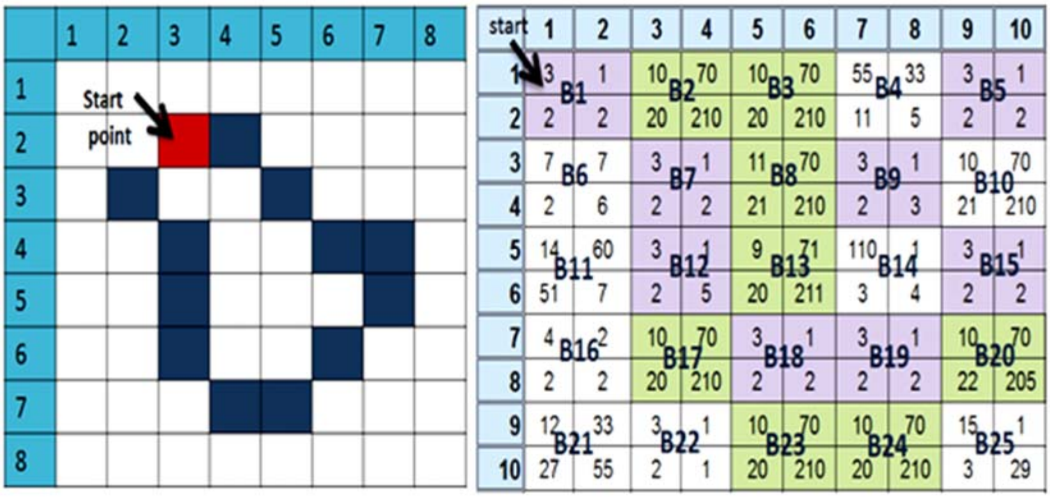


Figure 1. A. Chain code with 4- connectivity, B. Chain code with 8- connectivity.

The chain code of a segment can begin at any pixel on the boundary. It works to find the next adjacent pixel on the boundary in a clockwise direction by saving the direction between (zero to seven) in an output buffer and continuing the process from the next pixel. When we reach the starting pixel again, the chain code is complete. The output buffer has a set of direction values that include the chain code itself, and from which the original set of pixels can be recreated starting at any pixel position in an image. As an example, a chain code for the region with 8-connected is shown in figure 2-A. In this paper we develop the traditional chain code using Quadruple pixel (vector of 4 pixels), and find the chain code for image depending on one of the similarity measures that were used to find two Adjacent vectors that are almost alike [12]. Figure 2-B shows an example that illustrates how the Quad chain code computed an image.



A. The chain code with 8- connectivity in location(2,3) is 0,7,7,0,6,5,5,4,3,2,2,3

B. The Quad chain code with 8- connectivity The Quad chain code in location (1,1)is 7,6,7,0,1,3,2 Blocks B1,B7,B12,B18,B19,B15,B9,B5

Figure 2. The comparison between traditional chain code and Quad chain code (clockwise).

The similarity measures can be applied to find vectors (quad of pixels) that are more alike are (cosine similarity, jaccard similarity, Dice similarity) as illustrating in table 1 [13].

Table 1. The similarity measures

No	Similarity measure	Actual formula	
1	Cosine	$\frac{A \cdot B}{\|\|A\|\| \ \|\|B\|\|}$	(1)
2	Jaccard	$\frac{A \cdot B}{\|\|A\|\|^2 + \|\|B\|\|^2 - A \cdot B}$	(2)
3	Dice	$2 \frac{A \cdot B}{\|\|A\|\|^2 + \|\|B\|\|^2}$	(3)

For example, if A and B as the vector, when A vector =(1,3,7,4) and B vector =(5,3,1,6) then the similarity measures are illustrated in table 2. When ||A|| is √(1*1+3*3+7*7+4*4), A·B means (1*5+ 3*3+7*1+4*6). As long as the similarity measure returns values in the range [0,1], when the similarity value is closer to 1 that mean blocks is more alike and Vice versa.

Table 2. Example of similarity measures

Cosine similarity	Jaccard similarity	Dice Similarity
0.61669	0.44554	0.61643

3.2. Discrete cosine transforms (DCT).

DCT is the most used transform in the image processing applications for feature extraction. The method includes taking the transformation of the whole image and splitting the related coefficients. The DCT of an image includes three frequency components that are low, middle and high each with some detail and information in an image. The low frequency contains the average intensity of an image [14]. Mathematically, the two dimension-DCT of an image is given by:

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (3)$$

for $u = 0,\dots,7$ and $v = 0,\dots,7$

where $C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$

The human eye is able to catch alterations to the lower frequencies since most of the image's frequency content is located in this area. Changing high frequencies can cause a multitude of local distortions along the image's sharp edges. To minimize distortion, the data should be added in the middle frequencies. Middle Frequencies are considered insignificant transform coefficients as thus set Threshold value in this space [15]. As Shown in figure 5:

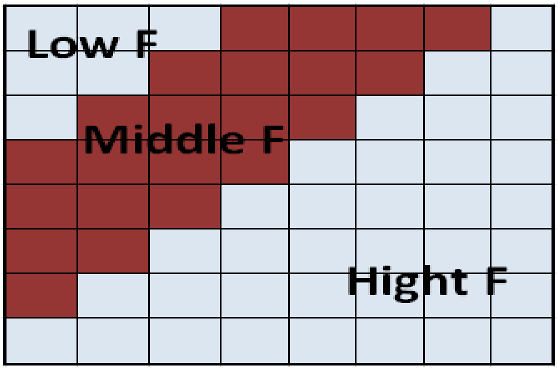


Figure 3. Frequency regions of DCT Coefficients

4. The proposed method.

The proposed method consists of two general stages (the message hiding process, the extract message process), each one contains many steps.

4.1. The message hiding process:

In this stage there are several steps as illustrated in Figure 4 of hiding a secret message in an image depending on quad chain code and DCT, it consist of:

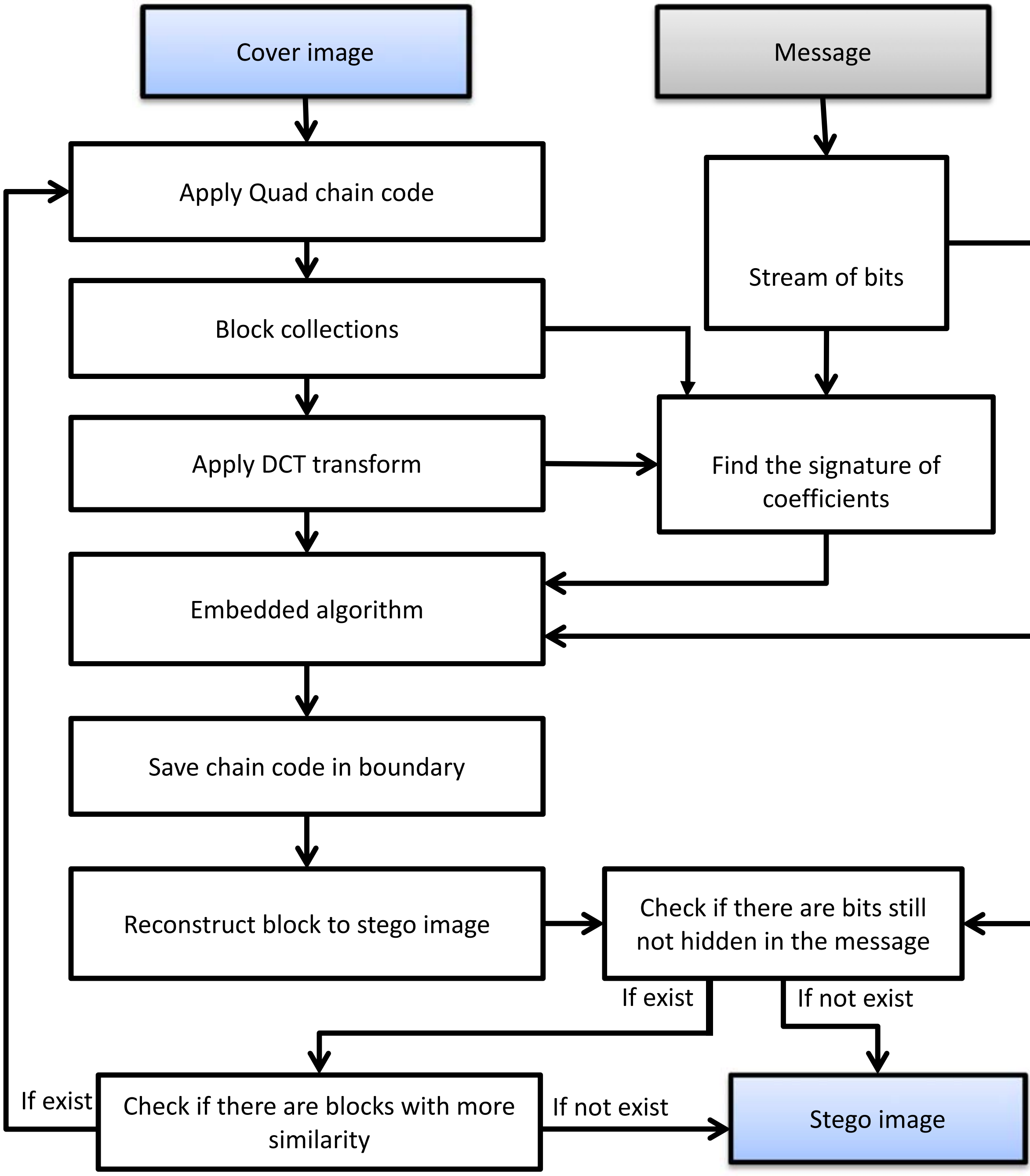


Figure 4. The block diagram of the message hiding stage.

4.1.1. Read the cover image and the secret message:

This step will choose an image to be a cover and read the message that we need to embed inside the cover image which is a gray-scale (8 bit per pixel).

4.1.2. Apply quad chain code.

This step will be applying the development chain code (quad chain code) to find quads of pixels (vectors, each vector consist of 4 pixels) that is more alike depended on one of the similarity measures (cosine similarity, jaccard similarity, Dice similarity). Quad chain code that was found by scanning the pixels of the cover image checks if there are (16) quads similar with each other to collect block with size 8*8 (16 quad pixels equal 64 pixel) in the next step, as shown in figure 5 .

Algorithm name: Quad chain code
Input: the cover image with 8 bit per pixel, similarity ratio.
Output: start point of chain code, stream of chain code as array in one dimension with size 15 cells.
1. **Begin**
2. Convert the cover image to matrix.
3 **For** i= 1 to the high of a cover image
4. **For** j=1 to the width of a cover image
5. . Let index1=i, index2=j, k =0.
6. **Repeat**
7. **If** there are adjacent quad pixels for location of the cover image matrix [index1, index2] that the similarity measure is largest than similarity ratio **AND** the current quad not visited **then**
8. **Begin**
9. Save chain code in chain matrix[k] with value between (0 - 7).
10. Update index1 and index2 depend on chain matrix[k].
11. k=k+1.
12. **Else**
13. k=0.
14. Go to the next quad pixels.
15. **End if**
16. **Until k<16**
17. Return start point and chain matrix.
18. **End for**
19. **End for**
End algorithm

Figure 5. Quad chain code algorithm.

4.1.3. Block collections.

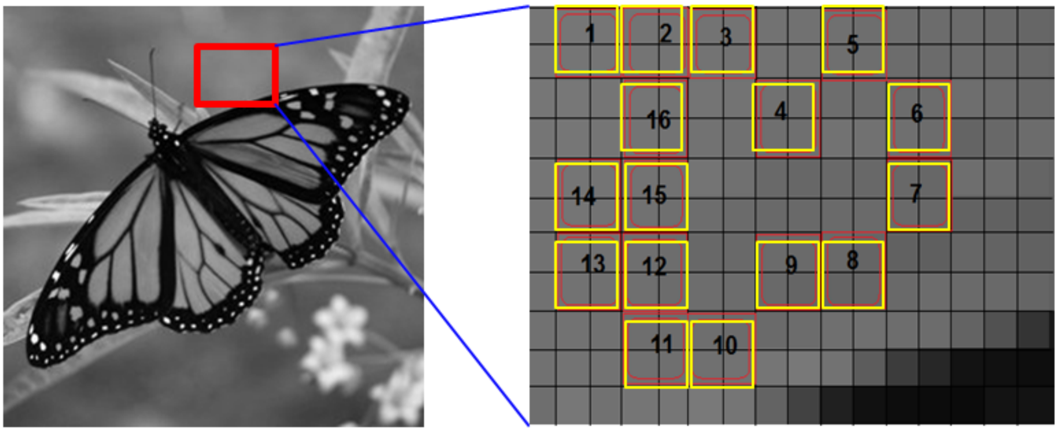
In this step, we will be collecting the quad pixels that were determined based on stream of chain code from the above step for equip block with size 8×8. Each quad pixel of the 8×8 block (16 Quad pixels, 64 pixels) is similar to each other, figure 6 explain how to collect block.

Algorithm name: Collect blocks.
Input: matrix of the cover image, start point of chain code, chain code matrix from above step.
Output: block with size 8x8
1. **Begin**
2. Save the first quad pixels in the block from matrix of the cover image in the location of start point.
3. Assigning special value (-2) to the current quad pixels in the matrix of the cover image.
4. i =0
5. **Repeat**
6. Update the location depending on chain matrix[i].
7. Save the next quad pixels in a block.
8. Assigning special value (-2) to the current quad pixels in a matrix of the cover image.
9. **Until i<16**
10. **Return** block with size 8*8.
End algorithm

Figure 6. Block collections algorithm.

4.1.4. Apply DCT Transform.

This step will be applying the 2D-DCT transform for blocks that were equipment from the above step to convert values of pixels from the spatial domain to the frequency domain.in this step we also convert the string message to a stream of bits. As shown in figure 7 which explain this process.



A. The cover image B. Apply Quad chain code for the cover image

118	118	118	119	119	119	118	119
118	119	118	118	118	118	120	118
119	118	120	119	119	118	118	117
119	120	120	119	118	118	118	117
117	118	118	118	119	120	119	119
118	118	118	118	118	120	118	118
118	117	119	119	118	117	119	118
119	117	120	118	119	116	118	118

C. Collect a block

947	-0.4	-1.2	0.5	-0.5	-0.9	0.2	-1
1	0	0	-0.7	-0.6	0.6	-0.7	1.2
-0.8	0.3	0.5	0.8	1.6	-0.6	-0.3	-1.2
-1	3	0.1	-1.3	-0.3	1	0.4	2.2
0.5	-0.1	-0.1	0.3	0.5	1	0.3	-0.1
0.2	-1.7	-0.6	0.8	0.5	-0.7	0.3	0.3
0	-0.7	-0.7	-0.6	0.7	0.5	1.6	0
0	1.5	-0.8	0.1	0.8	-0.2	0.4	-0.5

D. Apply 2D-DCT transforms

Figure 7. Some step of hiding operation

4.1.5. The signature of coefficients.

This step will be checking the number of bits (message) that can be embedded inside the block that was collected from step 4.1.3. The first operation is determined which locations of DCT coefficients have a zero value or values between (1,-1) Except the first row and the first column by using mask matrix with size 8*8, that means if each element of DCT coefficients between (1,-1) the corresponding value in mask matrix will be (1), otherwise the remaining values will be (0) .the bits of message must be hidden in some locations of corresponding spatial domain block that mask matrix is (1) by using least significant bit (LSB) algorithm .the strategy that is going to be applied is bottom- up. For Each hide operation to one of the block positions, we will find the DCT to block after hiding. Then we create the signature coefficients and compare them with the signature of coefficients that have been extracted in the beginning .we will continue the process of hiding bit after the other as long as there is no change in signature of coefficients, but must end the algorithm after the first change in the signature of coefficients, figure 8 explain the algorithm.

```
Algorithm name: signature of coefficients.
Input: B1 original block (8*8), DCT block (8*8), stream bits of the message.
Output: N number of bits can be embedded in the original block.
Begin
  Assign zero to all values of signature matrix1.
  Assign 1 to locations of signature matrix1 that are corresponding values of DCT block between (1,-1)
  N=0
  For i=7 to 1
    For j=7 to 1
      Insert one bit of the message in least significant bit of B1[i,j] location that is a corresponding value of
      Signature matrix1 is (1)
      Find DCT transform for B1 block after hiding
      N=N+1
      Assign zero to all values of signature matrix2.
      Assign 1 to locations of signature matrix2 that are corresponding values of DCT block between (1,-1)
      X= subtracting between signature matrix1 and signature matrix2
      If X <> 0 then
      Begin
        Return N
        End algorithm
      End if.
    End for
  End for
  Return N
End algorithm
```

Figure 8. The Signature of coefficients algorithm.

4.1.6. Embedded algorithm.

From the above step, we determine the number of bits that can be embedded in a block. This step will hide stream of bits in least significant bit of the block pixels from bottom to up (that means the initial hiding of a block will be in location (7,7) and We continue until we reach location (1,1)).

4.1.7. Save chain code in boundary.

After the hiding operation for each block, we save the stream of chain code in the first two boundary of the stego image. If the size of the cover image is 200*200 then that means it found 1584 locations (the first boundary has 796 (200+199+199+198), the second boundary has 788 locations (198+197+197+196)) that were used to save chain code for each block that has the hidden operation in it. The number of blocks that contain hidden bits will be saved in the 4 corner locations of stego image (embedded two bits for each corner location by using LSB algorithm, these locations are [0,0],[0,199],[199,199],[199,0]) .the stream of chain code(with size 15 for each block) will be embedded in the first boundary of the stego image except the corners, we note the values of chain code between (0-7) need 3 bits to be represented, then we need to embed 3 bits for each pixel in the first boundary of the stego image . The second boundary will be used to hide the start point [i,j] of each block and number of bits that were embedded in the block. We note that there are 3 values (i, j, no of bits) for each block, these values will be converted to binary bits with 10 digits, so the start point of chain code and number of bits will be converted to (30) bits and hide these bits in the second boundary that is corresponding to the hidden chain code of a block in the first boundary This step will help in the extracting message stage.

4.1.8. Reconstruct block to the stego image.

This step will be reconstructing blocks to the stego image by assigning new values of pixels after hidden bits of a message depending on the stream of chain code for each block. After this operation there will be a check if there are bits in a message still not hidden, if yes there will be another check if the quad pixels in the cover image that are more similarity with each other are found, if yes then go to the step 4.1.2. Otherwise, end the algorithm and the stego image is ready to be sent to the destination.

4.2. The extract message stage.

In this stage there are several steps as illustrated in Figure 9 to extract a secret message from the stego image depending on quad chain code and DCT, it consist of:

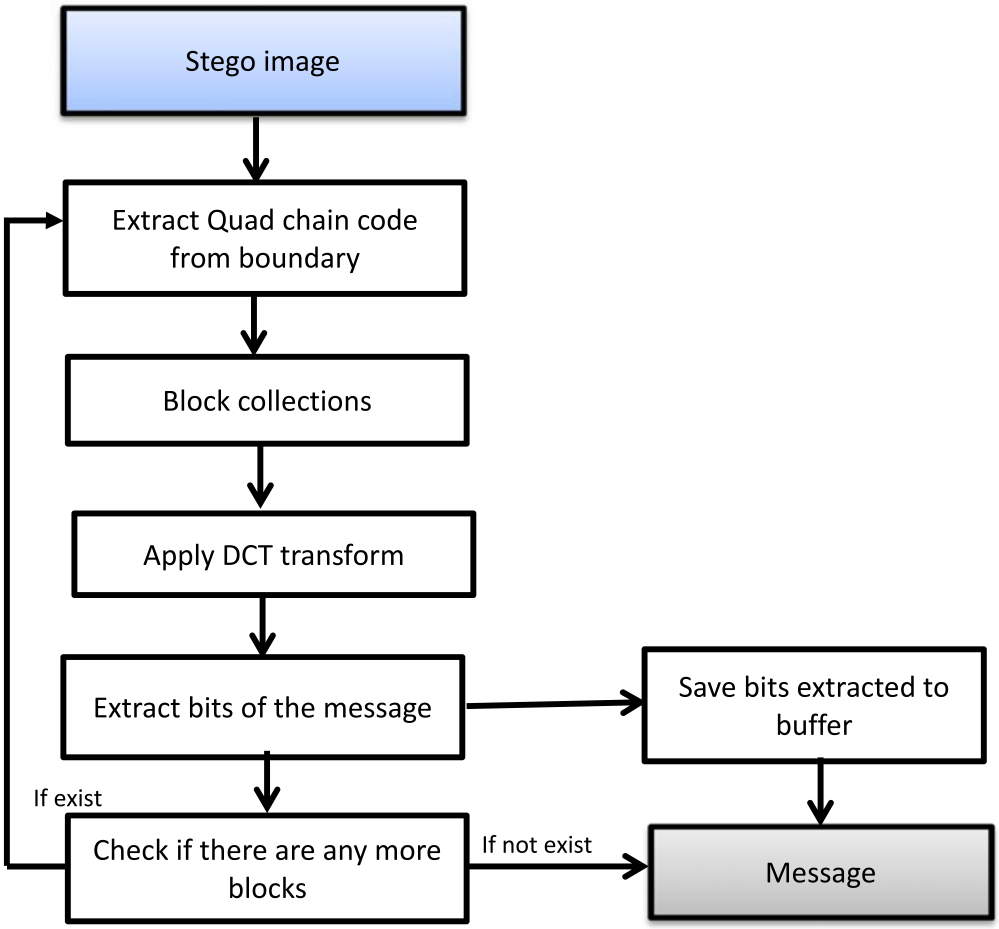


Figure 9. The block diagram of extract message stage.

4.2.1. Extract Quad chain code from boundary.

The first operation in this step is read the stego image and extract the number of blocks from the values in corners locations of stego image by take the two least significant bits and merge this bits to converted from binary to decimal value that determine which obtain the hiding number of bits in the first stage. Depending on this value will be reading the pixels from the second boundary of stego image and extract the two least significant bits for each pixel to merging these bits to find the start point and the number of bits for each block. The stream of chain code will be extracting from the first boundary of stego image by taking the last three bits for each pixel to find values between (0-7).

4.2.2. Block collections.

This step will be taking values of quad pixels from stego image to equipment block with size 8*8 depending on start point of a block and the stream of chain code that were extracted from the above step.

4.2.3. Apply DCT transform.

This step will be applying the DCT transform for the block that was extracted from the above step.

4.2.4. Extract bits of the message and save it extracted to buffer.

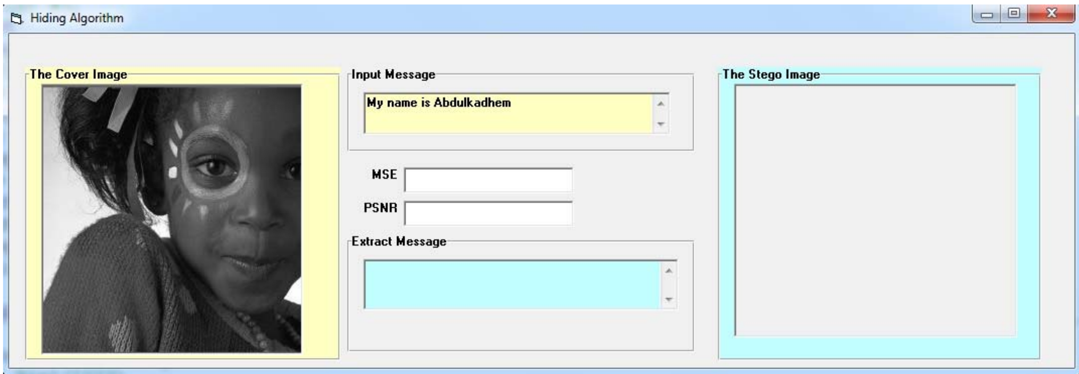
Depending on the number of bits that were extracted in step 4.2.1, we must extract the least significant bits of the pixels values of block from the bottom to up .the extracting bits will be saved in the buffer.

4.2.5. Extracting message.

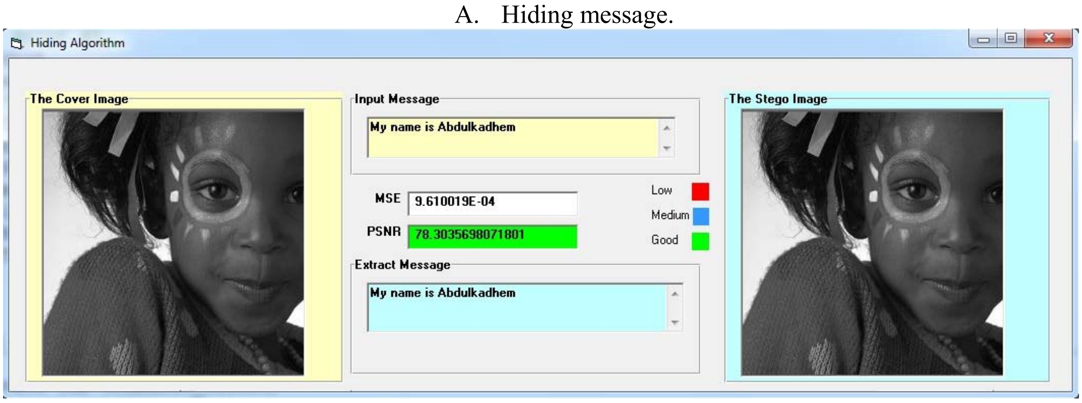
The above steps are continued till covering all blocks depending on the number of blocks in location (0,0) and save the bits in the buffer. Finally, the stream of bits in the buffer will be converted to a message.

5. Experimental results.

Experiments of the proposed method in this paper are carried out to prove the efficiency. The proposed method has been simulated using the visual basic 6.0 program on Windows 7 platform. Figure 10 shows the interface system of hiding and extracting process.



A. Hiding message.



B. Extracting message.

Figure 10. Interface system of hiding algorithm.

Figure 11 shows a set of 8-bit grayscale images of size 256 × 256 are used as the cover image to form the stego-image.

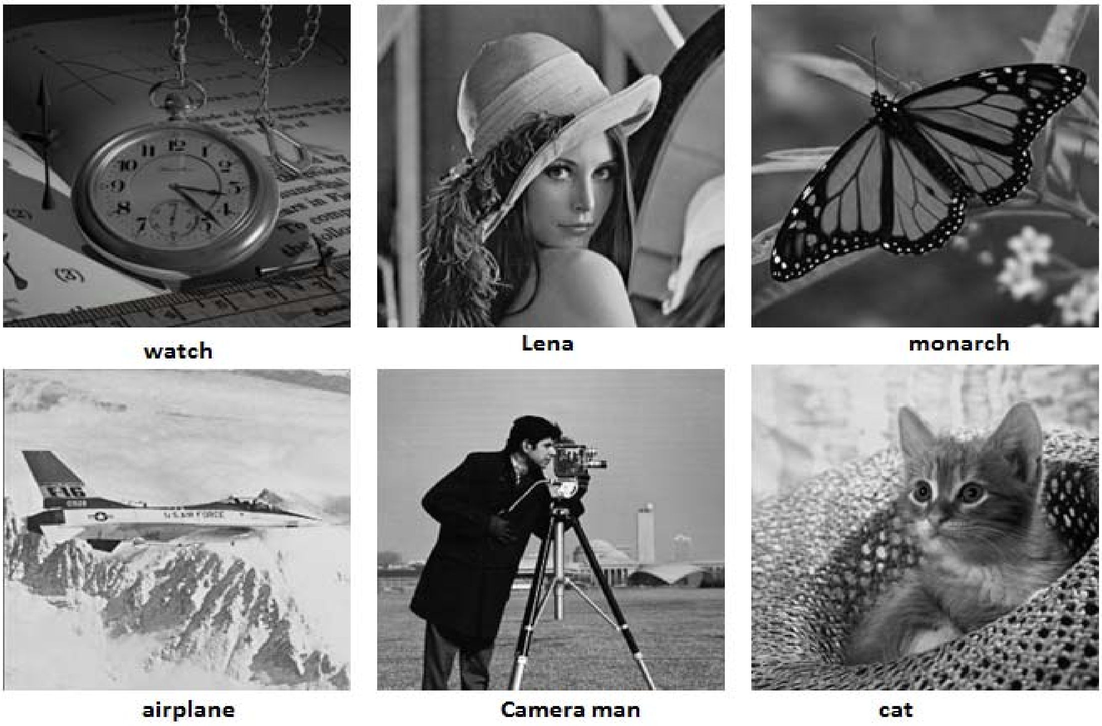


Figure 11. Some grayscale images of size 256 × 256.

The similarity measure that are used for above images is (cosine measure) and the similarity ratio (threshold) is 95% between quads of pixels. The quality of the stego image is measured through the mean square error (MSE) that returns cumulative squared error between the cover image and the stego image and the Peak Signal to Noise Ratio (PSNR) that returns the ratio of the maximum signal to noise between two images(cover, stego), in decibels. The best values of error measures are when the MSE is low and the PSNR is large. The mathematical equation for this error measures are:

$$MSE(cover, stego) = \frac{\sum_{i=0}^{N-1} \sum_{j}^{M-1} (cover(i,j) - stego(i,j))}{N \times M} \quad (5)$$

$$PSNR(cover, stego) = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad (6)$$

Where N, M are the dimensions of the cover image and stego image. Table 3 explains the MSE and the PSNR value of stego images for the proposed method of hiding message in the image depending on the quad chain code and DCT.

Table 3. The MSE and the PSNR value of stego images for the proposed method

images	MSE without boundary	PSNR without boundary	MSE with boundary	PSNR With boundary	Similarity Ratio
watch	0.000806	79.06745	0 .310135	53.215295	95%
Lena	0.000356	82.60412	0 .371002	52.437041	95%
monarch	0.000790	79.14903	0 .287872	53.538809	95%
airplane	0.000512	81.03810	0 .255676	54.053903	95%
cameraman	0.000543	80.78280	0 .422607	51.871436	95%
cat	0 .000574	80.541684	0 .592804	50.401692	95%

6. Conclusion

In this paper, we present a new algorithm for steganography depending on quad chain code and DCT. This algorithm gives a good robust against the attacker because the methodology of an algorithm based on randomization. The Randomization comes from three directions, the first one is applying quad chain code that select quad pixels which are not sequential but randomly (may take the zigzag shape), the second one is applying the DCT transform to find what location gives zeros values (between 1,-1), the third one is applying signature coefficients algorithm which is used to determine number of bits in the message that can be embedded in a block.

7. References

[1] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", International Journal of Computer Applications, vol 72, no.17,pp.39-44, June 2013.
[2] Hardik Patel, Preeti Dave, "Steganography Technique Based on DCT Coefficients", International Journal of Engineering Research and Applications (IJERA), vol. 2, no. 1, pp.713-717, 2012.
[3] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "A novel technique for image steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, vol. 2, no. 3, pp. 103-112, 2010.
[4] Komal Patel, Sumit Utareja, Hitesh Gupta, "A Survey of Information Hiding Techniques", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no.1, pp. 347-350, 2013.
[5] Tawfiq A. Al-Asadi, Ali Abdul Azzez Mohammad Baker, "A Novel Method for Image Steganography Based on Texture Features ", EUROPEAN ACADEMIC RESEARCH vol. 2, no. 1,pp193-203, 2014.
[6] Nor Amizam Jusoh, Jasni Mohamad Zain, "Application of freeman Chain Codes: An Alternative Recognition Technique for Malaysian Car Plates", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no.11, pp. 22-227, 2009.
[7] Prof. Dr. Tawfiq Abdulkhaleq Abbas, Fanar Ali Joda, " Locational Image Compression based on Chain Code Representation", IOSR Journal of Engineering (IOSRJEN), vol. 4, no. 1, pp. 24-29 2014.
[8] Bhavana.S, and K.L.Sudha, "TEXT STEGANOGRAPHY USING LSB INSERTION METHOD ALONG WITH CHAOS THEORY", International Journal of Computer Science, Engineering and Applications (IJCSEA), vol.2, no.2, pp. 145-149, 2012.
[9] Zuheir H.Ali, "information hiding Using Chain code technique ", Al-Turath University College Magazine, vol. 1, no. 9, pp. 44-55, 2010.
[10] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattanaik, " BIT LENGTH REPLACEMENT STEGANOGRAPHY BASED ON DCT COEFFICIENTS ", International Journal of Engineering Science and Technology, vol. 2, no. 8, pp. 3561-3570, 2010.
[11] Shahana T, "A Secure DCT Image Steganography based on Public-Key Cryptography ", International Journal of Computer Trends and Technology (IJCTT), vol. 4, no. 7, pp. 2039-2043, 2013.
[12] Tawfiq A. Al-Asadi, Israa Hadi Ail, Abdul Kadhem Abdul Kareem Abdul Kadhem, " Determine Blocks of Image for Hiding Operation Based on Quad Chain Code and DCT", EUROPEAN ACADEMIC RESEARCH, vol. 2, no. 10, pp. 12678-12689, 2015.
[13] Vikas Thada, Dr Vivek Jaglan , "Comparison of Jaccard, Dice, Cosine Similarity Coefficient To Find Best Fitness Value for Web Retrieved Documents Using Genetic Algorithm" ,International Journal of Innovations in Engineering and Technology (IJIET), vol. 2 no. 4, pp. 202-205, 2013.
[14] K Manikantan, Vaishnavi Govindarajan, V V S Sasi Kiran, S Ramachandran," Face Recognition using Block-Based DCT Feature Extraction", Journal of Advanced Computer Science and Technology, vol. 1, no. 4, pp. 266-283, 2012.
[15] Tribhuwan Kumar Tewari, Vikas Saxena, S Ramachandran , "An Improved and Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications, vol. 3, no. 1, pp. 28-32, 2010.